

LA-UR-21-23061

Approved for public release; distribution is unlimited.

Title: Initial Security Briefing

Author(s): Williams, Karen Elizabeth

Intended for: Security Presentation that will be shared/released outside of LANL.

Issued: 2021-03-30

Disclaimer:

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.



Initial Security Briefing

Personnel Security (SEC-PS)

March 2021



Introduction

Security Awareness Coordinator: Karrie E. Williams
Group Leader (SEC-PS): Deborah Martinez



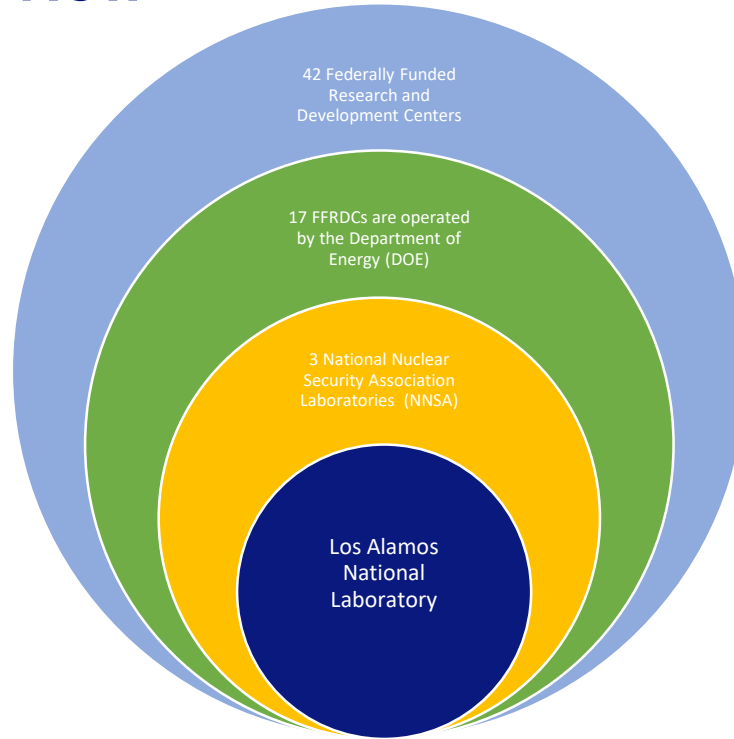


Objectives

- Introduce the various aspects of security at Los Alamos National Laboratory
- Understand the role of security in your work
- Know where to get answers to security related questions



Laboratory Overview



17 National Laboratories in 17 Minutes (Video):

https://www.youtube.com/watch?v=U63oRg59nxY&feature=emb_rel_end

Los Alamos National Laboratory

Mission:

To solve national security challenges through scientific excellence.





Defense Security Program (DFS)

DFS is the organization responsible for security at Los Alamos National Laboratory. It serves to enable the Laboratory to achieve its national security and science mission. DFS is responsible for preventing and neutralizing threats to the laboratory.

Office of Classification	Safeguards	Security
<ul style="list-style-type: none">•DFS-CL	<ul style="list-style-type: none">•OPSEC•Deployed Security•Nuclear Materials Control and Accountability•Planning and Analysis	<ul style="list-style-type: none">•Personnel Security•Physical Security•Security Investigations Team•Protection Program Operations•Classified Matter Protections and Control•Export Control



I. Moving Through The Laboratory



Access Control



Security Areas



Controlled and Prohibited Articles

Badge Types

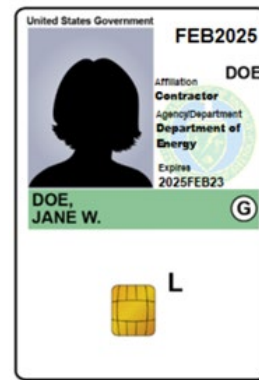
LANL-Issued Local Site Specific Only Badges



LSSO US Citizen Badges



LSSO Foreign National Badges



PIV Badge





Badge Responsibilities

- Your badge is required to conduct work on site. It must be worn photo-side out, above the waist, on the front side of the body at all times while on Laboratory property.
- Remove the badge and protect it from public view when leaving Laboratory premises.
- The badge must be used for official government purposes only; it is not meant to serve as an alternate form of identification.
- Do not photograph or photocopy your badge.
- Badges are intended for use only by the individual issued the badge. Do not share your badge.
- Limit the number of times you are issued a temporary badge.
- Badges are government property. Do not deface, destroy or otherwise alter any LANL-issued badge.
- Lost badge? Report within one business day to the Badge Office. Stolen Badge? Report ASAP to the Badge Office and the Security Incident Team (SIT) 505-665-3505
- Return the badge when access is no longer required/authorized
- Badges must be presented at the request of Protective Force, line management or the Personnel Security Group.
- You will be directed to **renew** your badge if:
 - your physical appearance significantly changes
 - your name legally changes,
 - clearance status changes
 - badge authorization expires
 - if your badge becomes damaged/demagnetized.



Security Areas [P202-1]

➤ General Access Areas (GAAs)

GAAS are open to all workers and the public during normal business hours. No identification/badge are required to enter a GAA during normal business hours. Privately owned vehicles (POVs) are permitted to enter GAAs.



➤ Property Protected Areas (PPAs)

PPAs are established to protect workers, facilities and property. For unescorted access into PPAs, personnel must possess a Department of Energy (DOE) security badge or a LANL-issued (LSSO) badge.



Security Areas



➤ Limited Areas (LAs)

Limited Areas are security areas established for the protection of classified matter and/or Category III Special Nuclear Material. For unescorted access into LAs, personnel must hold an active L or Q security clearance, unless more stringent controls are implemented. Personally owned vehicles are not permitted in LAs.

➤ Special Access Limited Areas (SALAs) and Q-Only LAs

SALAs and Q-Only LAs are established according to the Laboratory mission. For unescorted access into SALAs or Q-Only LAs, personnel must hold an active Q security clearance.

➤ Sensitive Compartmented Information Facilities (SCIFS) and Special Access Program Facilities (SAPFs)

SCIFS and SAPFS are areas, rooms, groups of rooms or installations where Sensitive Compartmentalized Information is stored, used, discussed and/or processed.



Security Areas

➤ Protected Areas (PAs)



PAs are security areas established to protect Category II Special Nuclear Material and classified matter. PAs may also be established to provide a concentric security zone surrounding a Material Access Area. For unescorted access, personnel must hold an active L Clearance or higher. Privately owned vehicles are prohibited. All workers, vehicles, packages and hand-carried articles are inspected upon entering and exiting PAs.

➤ Material Access Areas (MAAs)

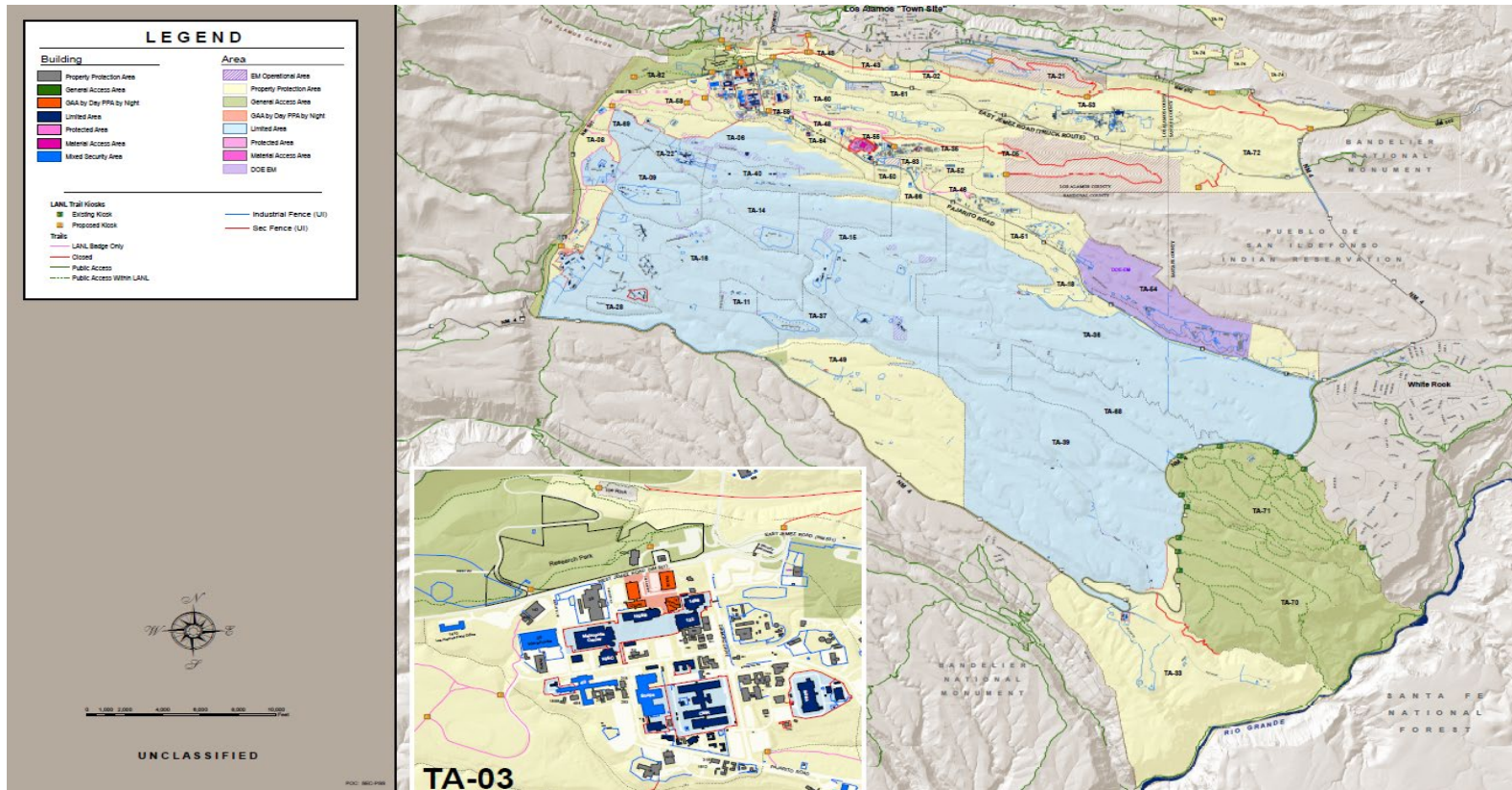


+ HRP

MAAs are security areas established to protect Category I and II Special Nuclear Material. MAAs must be located within a Protected Area. For unescorted access into an MAA, personnel must hold an active Q clearance and an active Human Reliability Program Certification. Privately owned vehicles are prohibited. All workers, vehicles, packages and hand-carried articles are inspected upon entering and exiting MAAs.



Physical Security Areas



Security Areas: Piggybacking and Tailgating

- “**Piggybacking**” occurs when an individual allows another individual to enter a badge reader controlled area without swiping their badge. This is also known as vouching and is categorically prohibited in badge reader controlled areas.
- “**Tailgating**” occurs when an individual follows another individual through a badge reader controlled area without the knowledge of that person.



Bottom Line:

Do not circumvent badge readers or other security measures.

Working at the Laboratory requires a certain level of awareness.

Report any known or suspected instances of piggybacking or tailgating to the Security Incident Team (SIT) 505-665-3505.



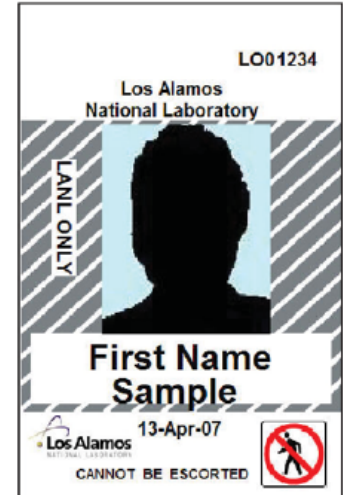
Security Areas: Escort Procedures



Until you are granted a security clearance (and sometimes even after!) your work may require you to be escorted into certain areas across the laboratory.

Some general guidelines while under escort:

- ✓ Stay with your assigned escort
- ✓ Properly display your badge at all times during the escort activity
- ✓ Escorting is not allowed into security areas for activities of a purely social nature.
- ✓ Check with your escort prior to introducing any electronic devices into a security area
- ✓ Individuals issued a “Do Not Escort” badge (right) may not be escorted into Limited Areas and above.



Challenging an Individual Without a Badge

If you notice an individual without a badge in a Property Protection Area or above, you may respectfully request they produce their badge. If the individual(s) is unable to produce a LANL-issued badge, they should be escorted out of the area and the Security Incident Team (505-665-3505) should be notified.

If you don't feel comfortable confronting an unbadged individual, let your responsible line manager (RLM) or Deployed Security Officer (DSO) know ASAP.





TAG YOUR BAG



Label all backpacks, duffel bags, lunch boxes, computer cases and purses with a bag tag- to include your name and a number where you can be reached.

Why?

Untagged bags left in public places at the Laboratory are assumed to be hazardous devices. If the owner cannot be located it will be turned over to Hazardous Devices Team for destruction.

Property of: _____

Phone #: _____



Photography, Bluetooth, and Wi-Fi

- Photography is prohibited anywhere on LANL property without prior approval.
- Bluetooth and Wi-Fi may only be enabled in General Access Areas (GAAs) with the exception of the LANL Wellness Center.



Controlled Articles

A controlled article, also known as a Portable Electronic Device (PED), is a device that is easily portable and can store, read, write, record, or transmit information. In general, personally owned PEDs are prohibited in Limited Areas and above. Government/LANL-issued mobile devices are also prohibited from entering “Secure Space.”



Includes (but is not limited to):

- Cellphones
- Tablets
- Smart Watches
- Cameras
- Laptops
- External Hard Drives
- Pagers
- Two-way Radios
- Medical Devices
- USB devices
- RFID enabled devices
- Wireless Earbuds



Prohibited Articles

The following items are **prohibited** on LANL property:

- Firearms
- Dangerous weapons / explosives (including ammunition, fireworks)
- Knives with a blade longer than 2.5 inches
- Alcohol
- Controlled Substances
- Drones / Unmanned Aircraft Systems
- Items prohibited by law

Reminder:

Introduction of a prohibited article into LANL property will result in a security incident and potential confiscation of the item by the Los Alamos Police Department.



III. Conducting Work Securely



Protective Force



Substance Abuse



Technical Surveillance Countermeasures



Protective Force

- One of the most visible elements of the Defense Security Program is the Protective Force (PF). The PF provides security services to the laboratory, including physical security for facilities, fixed and roving security patrols, access control and vehicle inspections, and security emergency response.
- Protective Force officers also staff Vehicle Access Portals at certain roadways coming into and within the laboratory. All vehicles are required to stop at the VAP and present identification.
- Canine Teams can also be seen– they deter and detect potential threats. Activities include explosive detection, suspect apprehension, and contraband searches.



Protective Force (Cont.)

- All vehicles and personnel on Laboratory property are subject to random personal and vehicle inspections. Certain areas, such as TA-55, will have more stringent security inspection requirements prior to entry.

Cooperation Requirements:

All personnel on Laboratory property are required to cooperate with PF officers on security matters and participate fully in the Laboratory's security programs.

Manhattan Era Security Check



Substance Abuse: Drug and Alcohol Testing

As a Department of Energy Laboratory with a national security mission, LANL cannot tolerate illegal activity and must ensure a work environment that is free from unauthorized or illegal use, possession or distribution of alcohol or controlled substances.

In support of the Laboratory's commitment to maintain a drug and alcohol-free workplace, **all** LANL badge holders are subject to regular drug and alcohol testing, to include:

- Pre-employment drug testing
- Random drug and alcohol testing
- Drug and alcohol testing based on reasonable suspicion
- Post-accident/post-incident drug and alcohol testing



If an individual fails to appear for a scheduled drug or alcohol test, the failure will be treated as a confirmed positive test.





Substance Abuse: Drug and Alcohol Use



The following **alcohol related** activities are prohibited:

- Consuming or possessing alcohol while on site, at Laboratory-sponsored functions.
- Consuming alcohol during scheduled work hours, including at lunch or while on break even if it is off-site.
- Testing at a breath alcohol result of .02 g/210 L or greater.

The following **drug related** activities are prohibited:

- Unlawful manufacture, dispensing, possession, use, transfer, or sale of drugs is prohibited, regardless of whether this occurs during work or on an individual's private time/property.
- Consuming marijuana remains prohibited under Federal Law.



Technical Surveillance Countermeasures

Technical surveillance countermeasures (TCSM) is an electronic countermeasures program used to detect and deter espionage, protect against inadvertent disclosure of classified or sensitive information, and protect your privacy at work.

Take the following steps if you suspect or become aware of a technical surveillance penetration:

- Do NOT remove or alter the suspected device
- Stop all classified processing and/or discussions
- Protect the area so that no one can remove the suspected device
- Immediately notify the TSCM Team via secure means and away from the compromised area
 - tscm_team@lanl.gov
 - 505-665-3409



II. Information Protection



Recognizing Classified Information

CUI

Controlled Unclassified Information



OPSEC



Recognizing Classified Information

- Federal law protects certain government information, documents, and material through the process of classification, which categorizes and ranks classified matter in proportion to the potential damage its unauthorized disclosure could cause to national security.
- Access to any level of classified matter is restricted to individuals who have a requisite **need-to-know** and the appropriate **access authorization** (security clearance).
- Classified information will be clearly affixed with markings indicating the category and level of sensitivity.

	Level		
Category	Top Secret (TS)	Secret (S)	Confidential (C)
Restricted Data (RD)	Q Only	Q Only	Q and L
Formerly Restricted Data (FRD)	Q Only	Q and L	Q and L
Transclassified Foreign Nuclear Information (TFNI)	Q Only	Q and L	Q and L
National Security Information (NSI)	Q Only	Q and L	Q and L
Degree of Damage	Exceptionally Grave	Serious	Undue Risk



Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) refers to unclassified information that is identified and marked as sensitive and subject to additional safeguarding.

Includes:

- Official Use Only (OUO)
 - Personally Identifiable Information (PII)
 - Export Control Information
 - **Limited to US Citizens only**
- Unclassified Controlled Nuclear Information (UCNI)
 - UCNI is certain information concerning nuclear facilities, materials, weapons and components
- Unclassified Naval Nuclear Propulsion Information (U-NNPI)
- Triad National Security, LLC Contractor Owned and Proprietary Information (TPI)



Controlled Unclassified Information

Access Requirements

- Need-to-know to perform official job duties

Additional Safeguards

- Ensure no unauthorized access
- When outside of a secured area, it must be stored in a locked receptacle
- Must be reproduced only to the minimum extent necessary
- Must be encrypted if being transmitted electronically
- Must only be destroyed by shredding or burning

Refer to LANL Policy 204-1 for more information.

OFFICIAL USE ONLY May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____ Department of Energy review required before public release. Name/Org: _____ Date: _____ Guidance (if applicable): _____
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. §2168 [2008]). Reviewing Official: _____ Date: _____ Guidance Used: _____ <small>(List all UCNi guidance used)</small>



RASSTI

- RASSTI (Review & Approval System for Scientific and Technical Information) is a system which assist LANL authors in reviewing documents leaving the Laboratory for and classified information or controlled unclassified information (CUI).
- You should submit documents through RASSTI for any Scientific & Technical Content (STI) carried out at the Laboratory with at least one LANL author that is being released outside the Laboratory.
- Email dchelp@lanl.gov if you are unsure if your document requires a RASSTI review.



OPSEC

Operations Security (OPSEC) is a security program that protects Laboratory information that is **neither** Classified or Controlled Unclassified Information (CUI).

OPSEC encourages employees to view operations from the perspective of an adversary in order to protect Critical Information. Critical Information are pieces of information that might:

- Assist an adversary in harming the Laboratory
- Prevent or impede the Laboratory from accomplishing its mission.

It is best to err on the side of caution when discussing laboratory activities in a public setting, even when those activities are unclassified.



OPSEC (VIDEO)



<https://www.youtube.com/watch?v=nlw2vdqVUXo>



Reporting



Personnel Security







Security Incidents



Incidents / Emergencies

Personnel Security

Please notify Personnel Security (SEC-PS) and/or Occupational Health (OSH-OH) **and** your Responsible Line Manager of the following circumstances:

- If you are arrested or convicted of any criminal drug statute violation clearance@lanl.gov
- If you are cited, arrested or convicted of any alcohol related incident (e.g., Driving Under the Influence [DUI], Driving While Intoxicated [DWI], public intoxication, open container, etc.) clearance@lanl.gov
- If you suspect you may have been exposed to any type of illegal drug. 
- If you are involved in a non-vehicular incident or accident at work that resulted in or had the potential to result in serious injury. 
- If involved in a vehicular accident while driving any government-owned vehicle or while on Laboratory property or Laboratory business. 
- If you are taking a legal drug that may impact your work performance 



Incidents of Security Concern

Incidents of Security Concern are actions, inactions or events which:

- Pose threats to national security interests or critical DOE assets;
- Create potentially serious or dangerous security situations;
- Degrade the effectiveness of the safeguards and security (S&S) programs;
- Adversely impact the ability of organizations to protect DOE S&S interests.

Examples include (but are not limited to):

- Mishandling of classified information
- Misuse of a LANL-issued security badge or computer system
- Introduction of a controlled/prohibited article
- Improper escorting



Incidents of Security Concern (cont.)

All LANL workers are required to immediately report any known or potential incidents of security concern to the Security Incident Team.

Report the potential IOSC immediately by calling the SIT

- Work hours: 505-665-3505
- After hours: 505-699-4094 (cell) 505-949-0156 (pager)



Report the incident to your Responsible Line Manager (RLM) and Deployed Security Officer (DSO)

Remember! When reporting a potential or known incident of security concern, do not discuss sensitive details over the phone. Simply state that you have a concern.



Emergency/Incident Reporting

ACTION—

Take out your phone and input the following phone number:
505-667-2400



The EOSC (Emergency Operations Support Center) is available to you 24 hours a day, 7 days a week, 365 days a year.

Using the Number:

Step 1: Call 9-1-1 for emergencies requiring police, fire or emergency medical support. Provide your location (Technical Area, Building and Room Number), injuries, explanation of alarms, what protective actions have been taken, and your name and call back number. Limit the use of acronyms.

Step 2: Call (505) 667-2400 Emergency Operations Support center.



Emergency/Incident Reporting



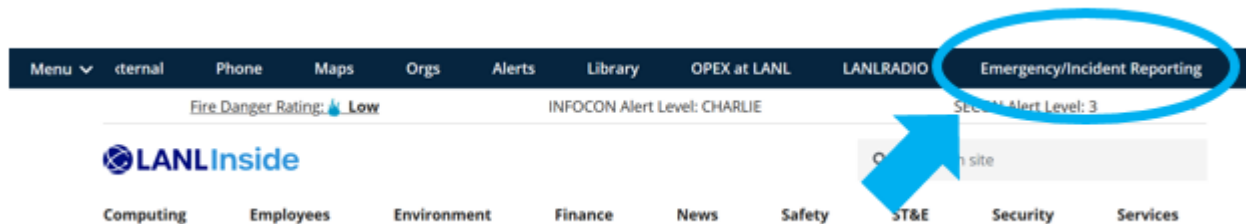
When to Report to the EOSC:

Examples of **Emergencies**:

- Fires or smoke odor
- Hazardous material release
- Suspicious packages or bomb threats
- Medical emergencies

Examples of **Non-Emergency** Incidents:

- Drones observed flying or landing on LANL property
- Wildlife concerns (bears, mountain lions, bats)
- Trespassing



Security Resources

Deployed Security Officer (DSO):

- <https://adss.lanl.gov/ds/Lists/DSOSPLContacts/AllItems.aspx>
- dso@lanl.gov

Personnel Security:

- (reporting) clearance@lanl.gov
- (substance abuse) 505-667-8378 (P-TEST)

Security Incident Team:

- Work hours: 505-665-3505
- After hours: 505-699-4094 (cell) 505-949-0156 (pager)

Emergency Operations Support Center

- 505-667-2400



Thank you for your attention
to your security training!



securityaware@lanl.gov

